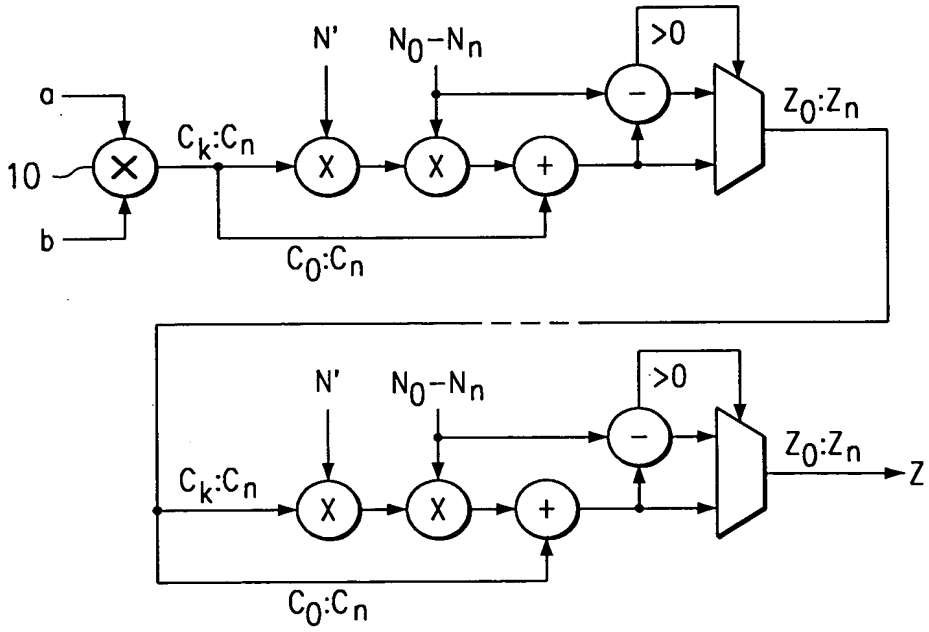
a
10
b
$C_k:C_n$
$C_0:C_n$
N'
N_0-N_n
>0
$Z_0:Z_n$
Z

FIG. 1

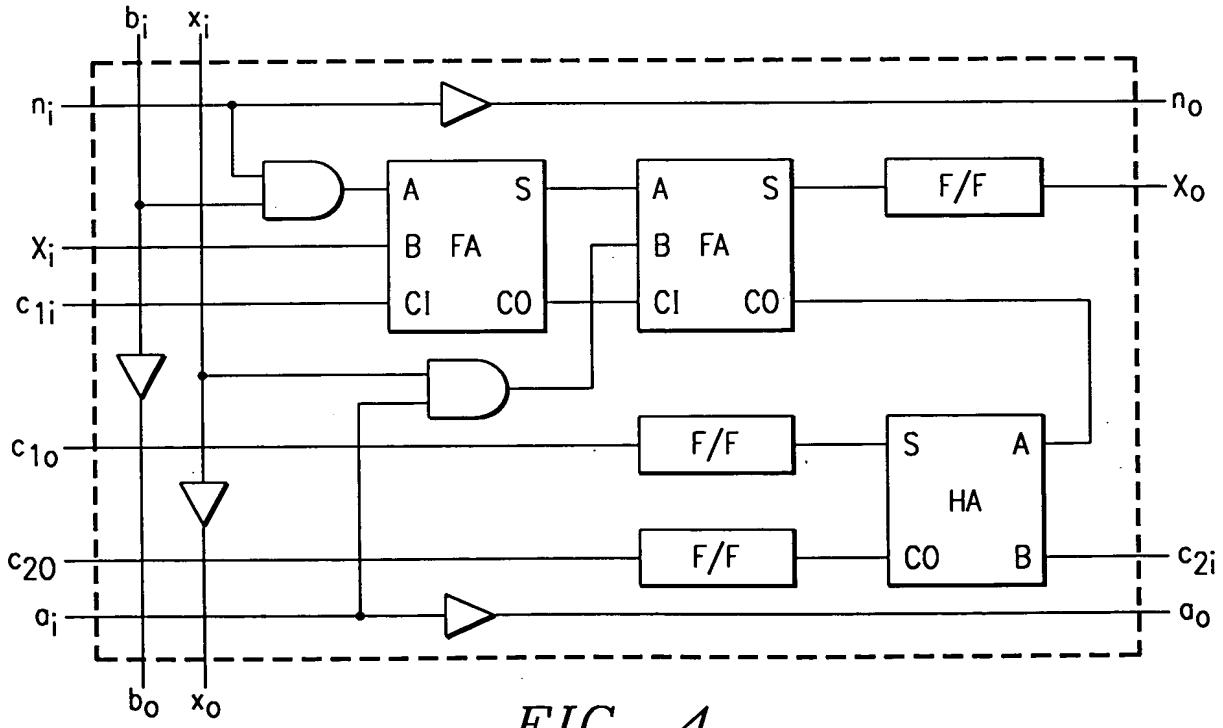
b_i
x_i
n_i
X_i
c_{1i}
c_{1o}
c_{20}
a_i
b_o
x_o
n_o
X_o
c_{2i}
a_o
A
B
CI
S
CO
FA
F/F
HA

FIG. 4

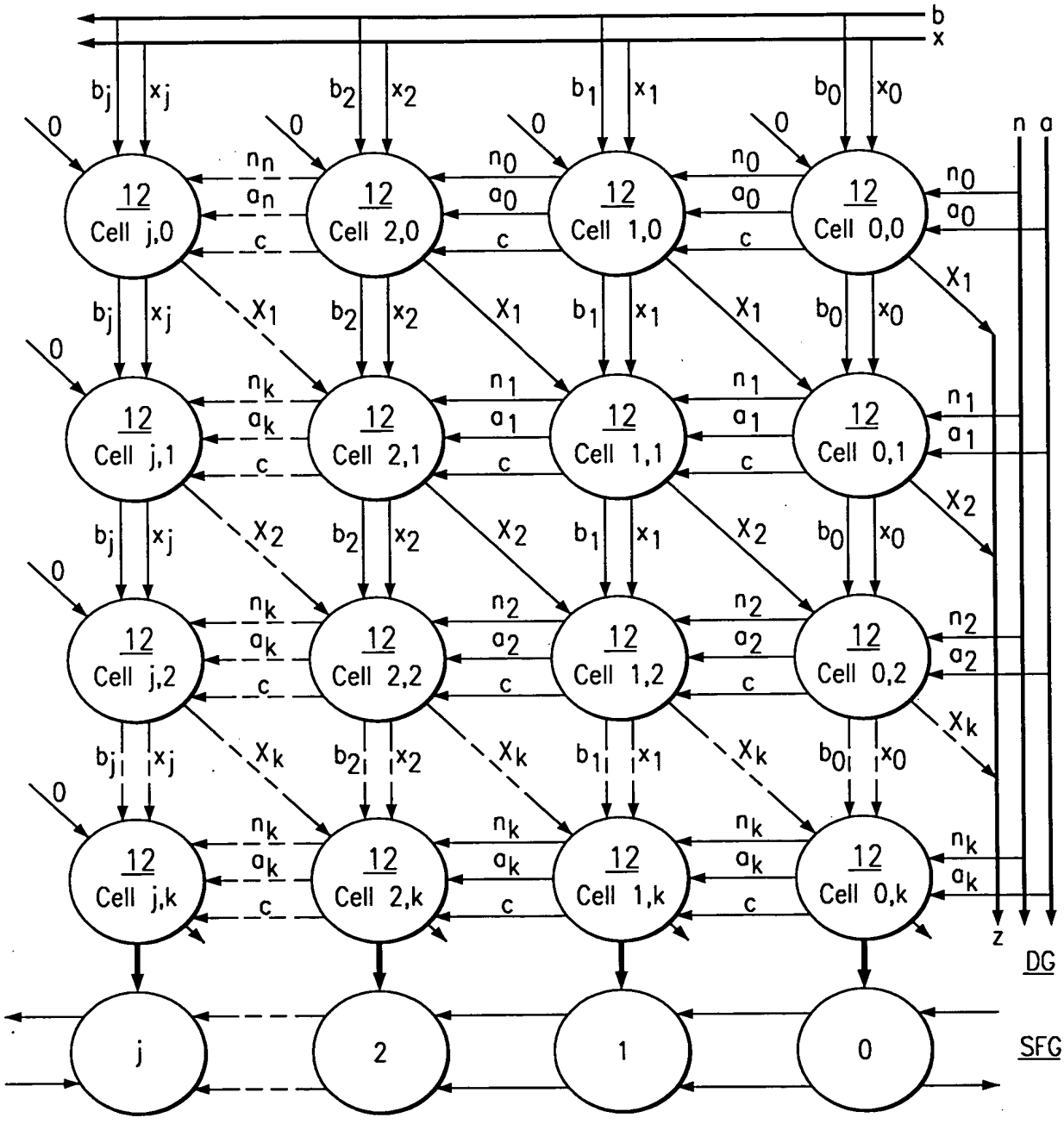
b
x
n a
12
Cell j,0
Cell 2,0
Cell 1,0
Cell 0,0
Cell j,1
Cell 2,1
Cell 1,1
Cell 0,1
Cell j,2
Cell 2,2
Cell 1,2
Cell 0,2
Cell j,k
Cell 2,k
Cell 1,k
Cell 0,k
z
DG
SFG
j
2
1
0

FIG. 2

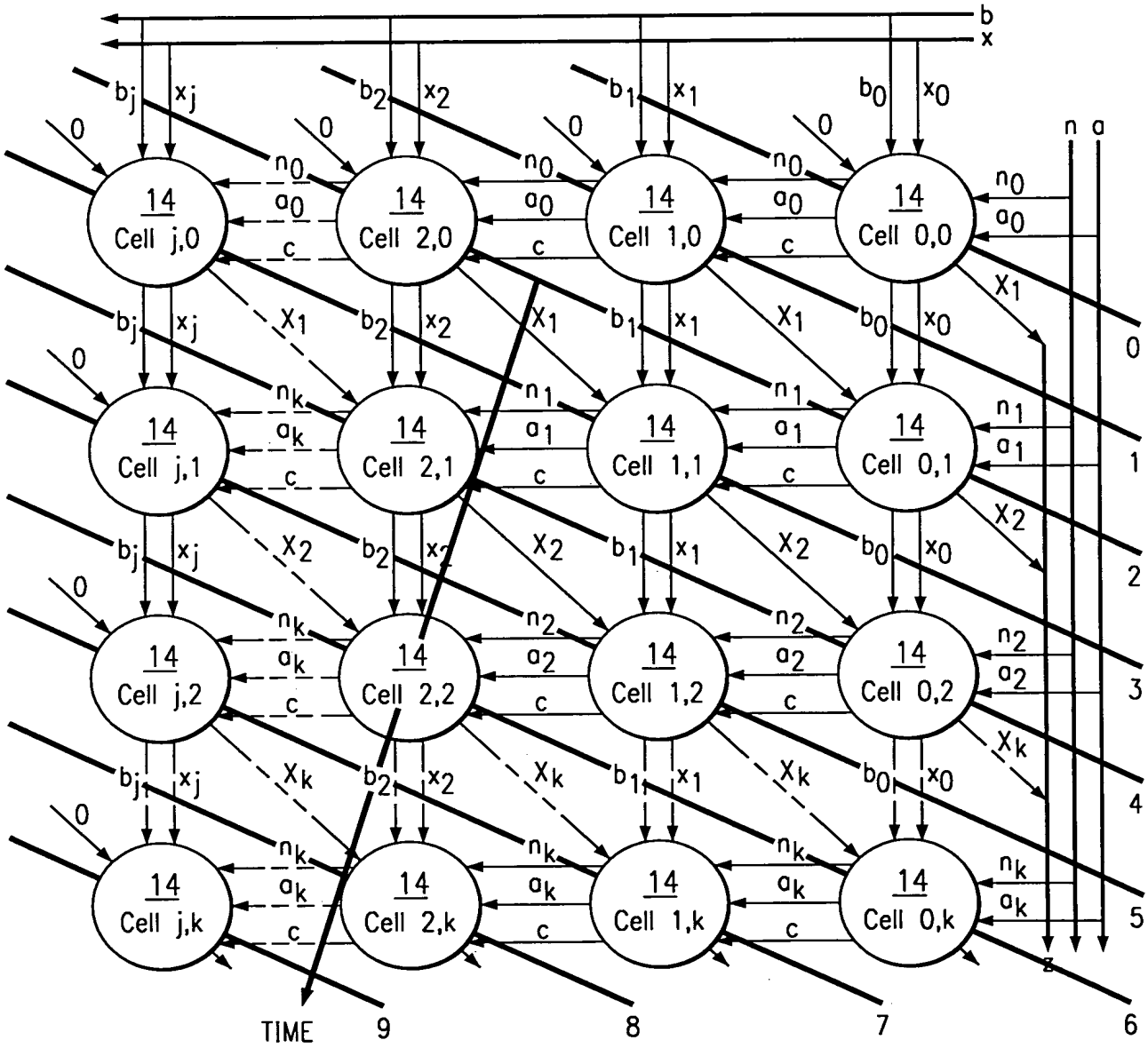
b
x
n a
14
Cell j,0
Cell 2,0
Cell 1,0
Cell 0,0
Cell j,1
Cell 2,1
Cell 1,1
Cell 0,1
Cell j,2
Cell 2,2
Cell 1,2
Cell 0,2
Cell j,k
Cell 2,k
Cell 1,k
Cell 0,k
TIME
0
1
2
3
4
5
6
7
8
9

FIG. 3

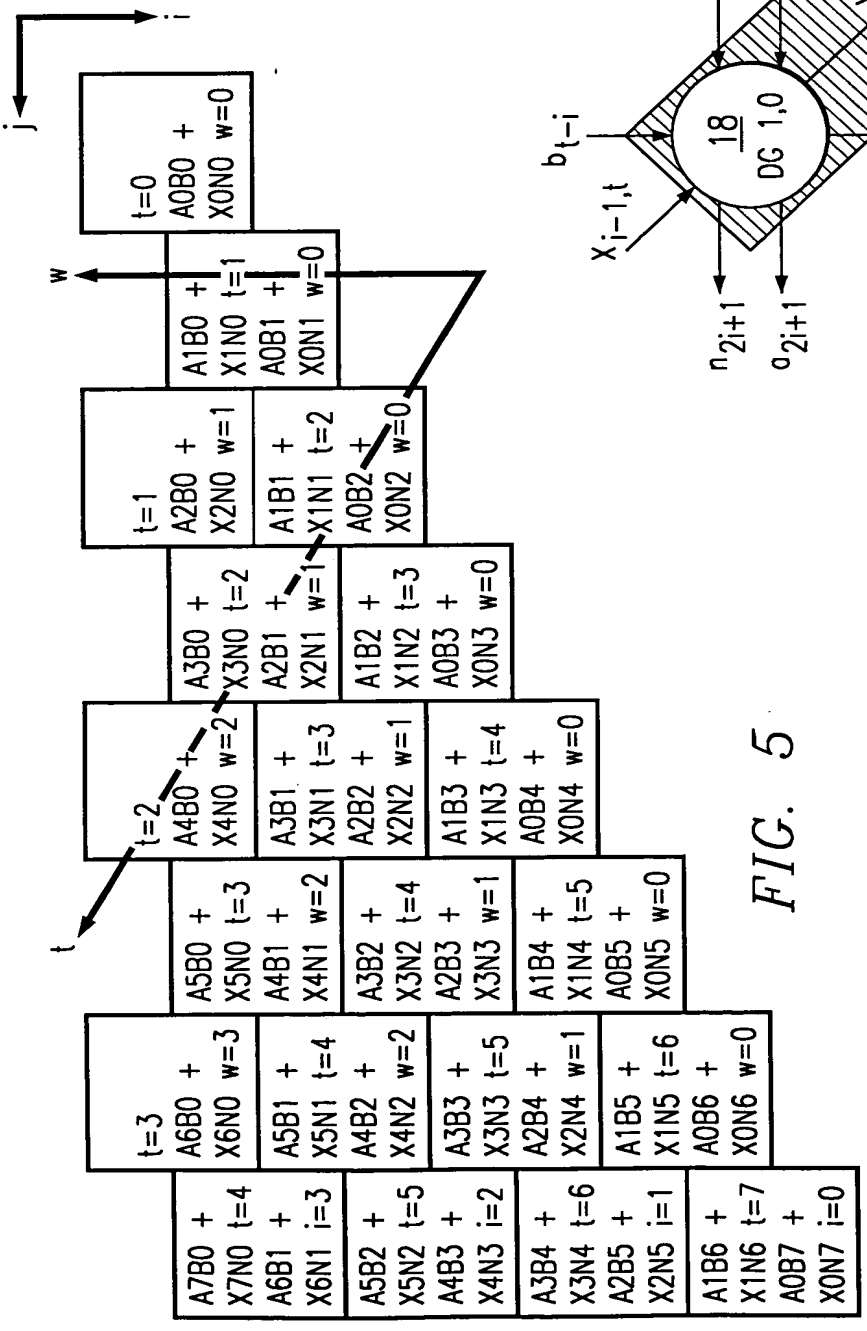
t=0 A0B0 + X0N0 w=0
t=1 A2B0 + X2N0 w=1
A1B0 + X1N0 t=1
A1B1 + X1N1 t=2
A0B1 + X0N1 w=0
t=2 A4B0 + X4N0 w=2
A3B0 + X3N0 t=2
A3B1 + X3N1 t=3
A2B1 + X2N1 w=1
A2B2 + X2N2 w=0
A1B2 + X1N2 t=3
A0B2 + X0N2 w=0
t=3 A6B0 + X6N0 w=3
A5B0 + X5N0 t=3
A5B1 + X5N1 t=4
A4B1 + X4N1 w=2
A4B2 + X4N2 w=1
A3B2 + X3N2 t=4
A3B3 + X3N3 w=1
A2B3 + X2N3 w=0
A1B3 + X1N3 t=4
A1B4 + X1N4 t=5
A0B3 + X0N3 w=0
A0B4 + X0N4 w=0
A7B0 + X7N0 t=4
A6B1 + X6N1 i=3
A5B2 + X5N2 t=5
A4B3 + X4N3 i=2
A3B4 + X3N4 t=6
A2B5 + X2N5 i=1
A1B6 + X1N6 t=7
A0B7 + X0N7 i=0
A0B5 + X0N5 w=0
A0B6 + X0N6 w=0
t
w
i
j

FIG. 5

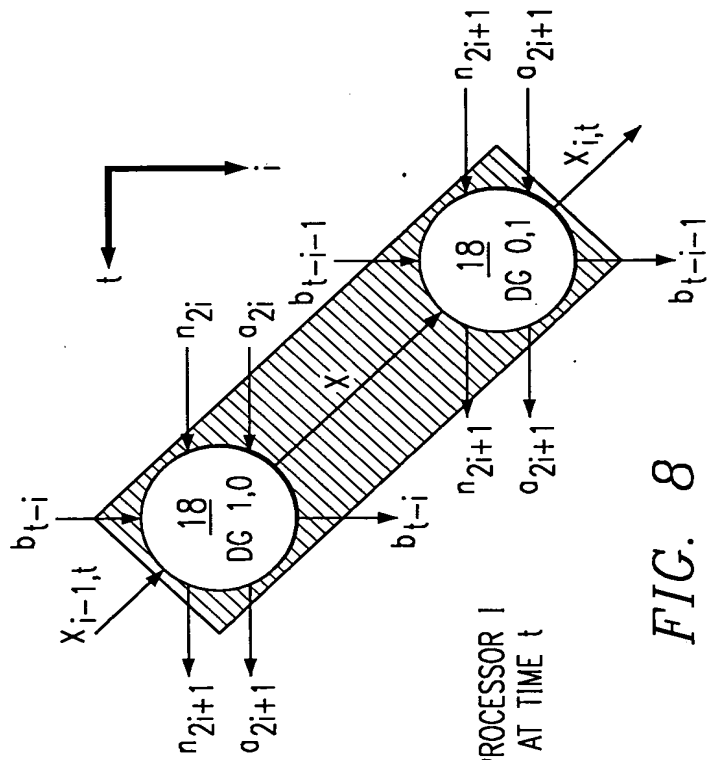
18
DG 1,0
18
DG 0,1
b_{t-i}
$X_{i-1,t}$
n_{2i}
o_{2i}
n_{2i+1}
o_{2i+1}
b_{t-i-1}
$X_{i,t}$
PROCESSOR I
AT TIME t
t
i

FIG. 8

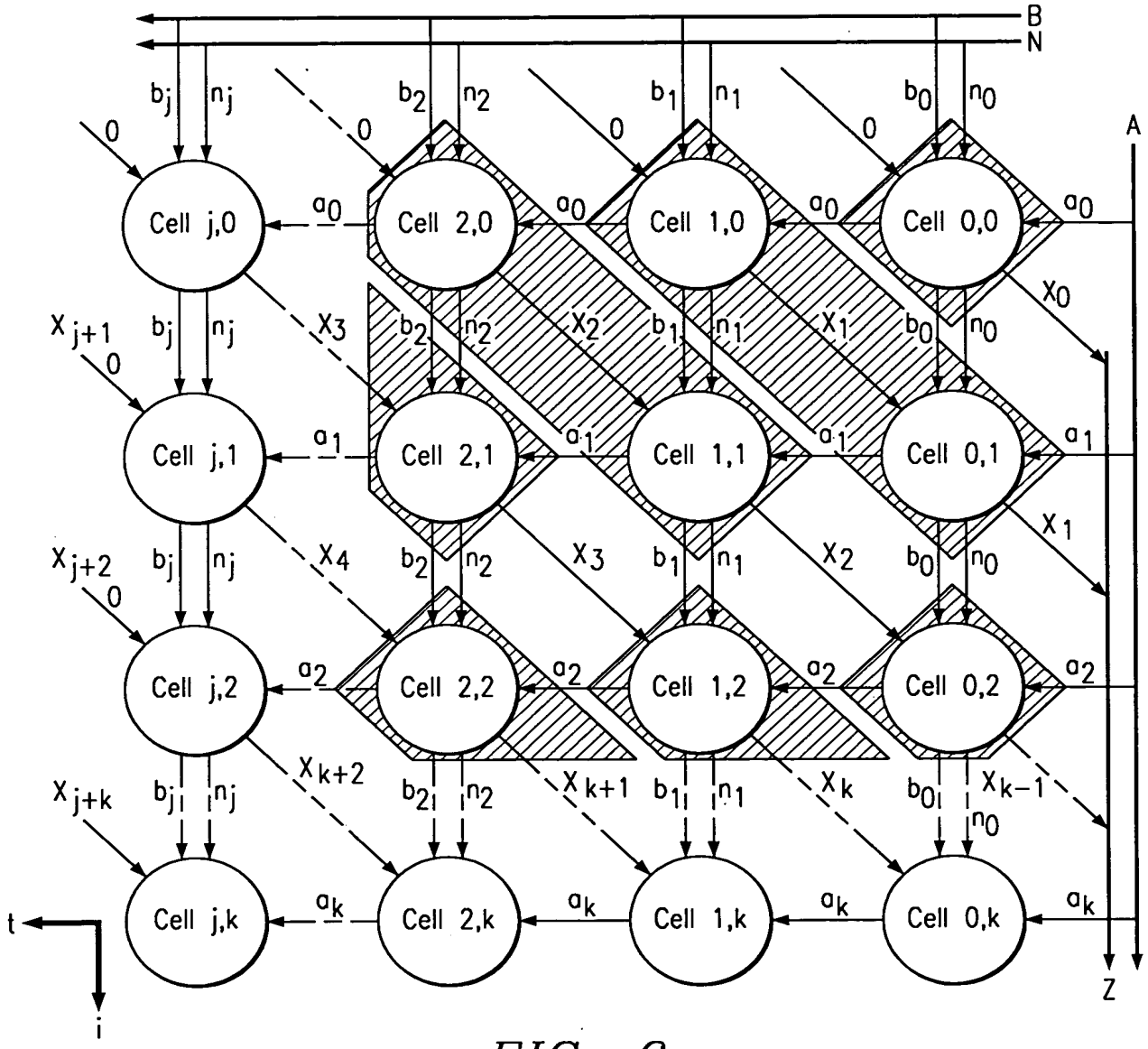
B
N
A
Z
t
i
Cell j,0
Cell 2,0
Cell 1,0
Cell 0,0
Cell j,1
Cell 2,1
Cell 1,1
Cell 0,1
Cell j,2
Cell 2,2
Cell 1,2
Cell 0,2
Cell j,k
Cell 2,k
Cell 1,k
Cell 0,k
0
b_j n_j
b_2 n_2
b_1 n_1
b_0 n_0
a_0
a_1
a_2
a_k
X_{j+1}
X_{j+2}
X_{j+k}
X_0
X_1
X_2
X_3
X_4
X_{k-1}
X_k
X_{k+1}
X_{k+2}

FIG. 6

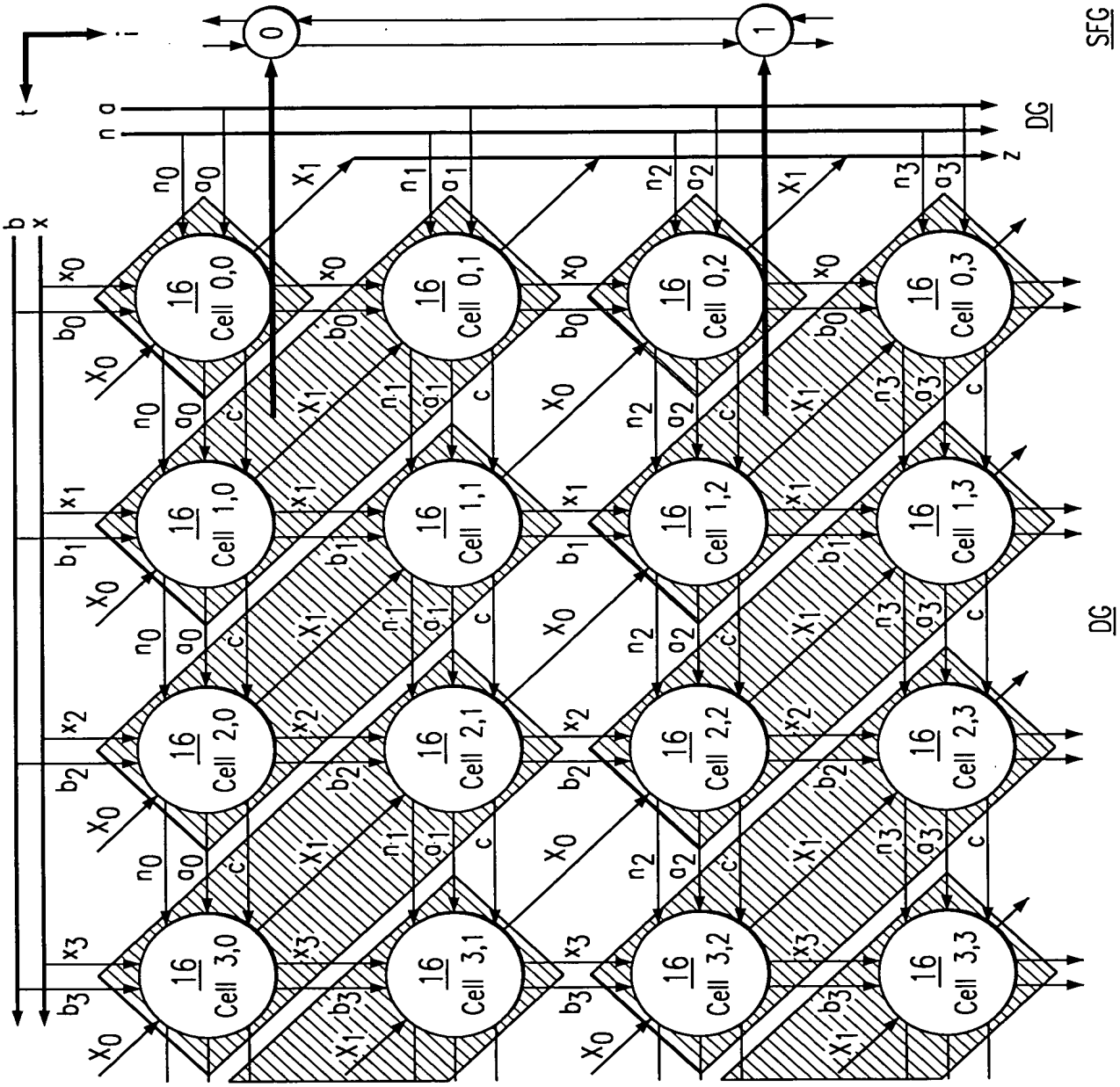
i
t
n a
b
x
z
DG
SFG
0
1
16
Cell 0,0
Cell 0,1
Cell 0,2
Cell 0,3
Cell 1,0
Cell 1,1
Cell 1,2
Cell 1,3
Cell 2,0
Cell 2,1
Cell 2,2
Cell 2,3
Cell 3,0
Cell 3,1
Cell 3,2
Cell 3,3

FIG. 7

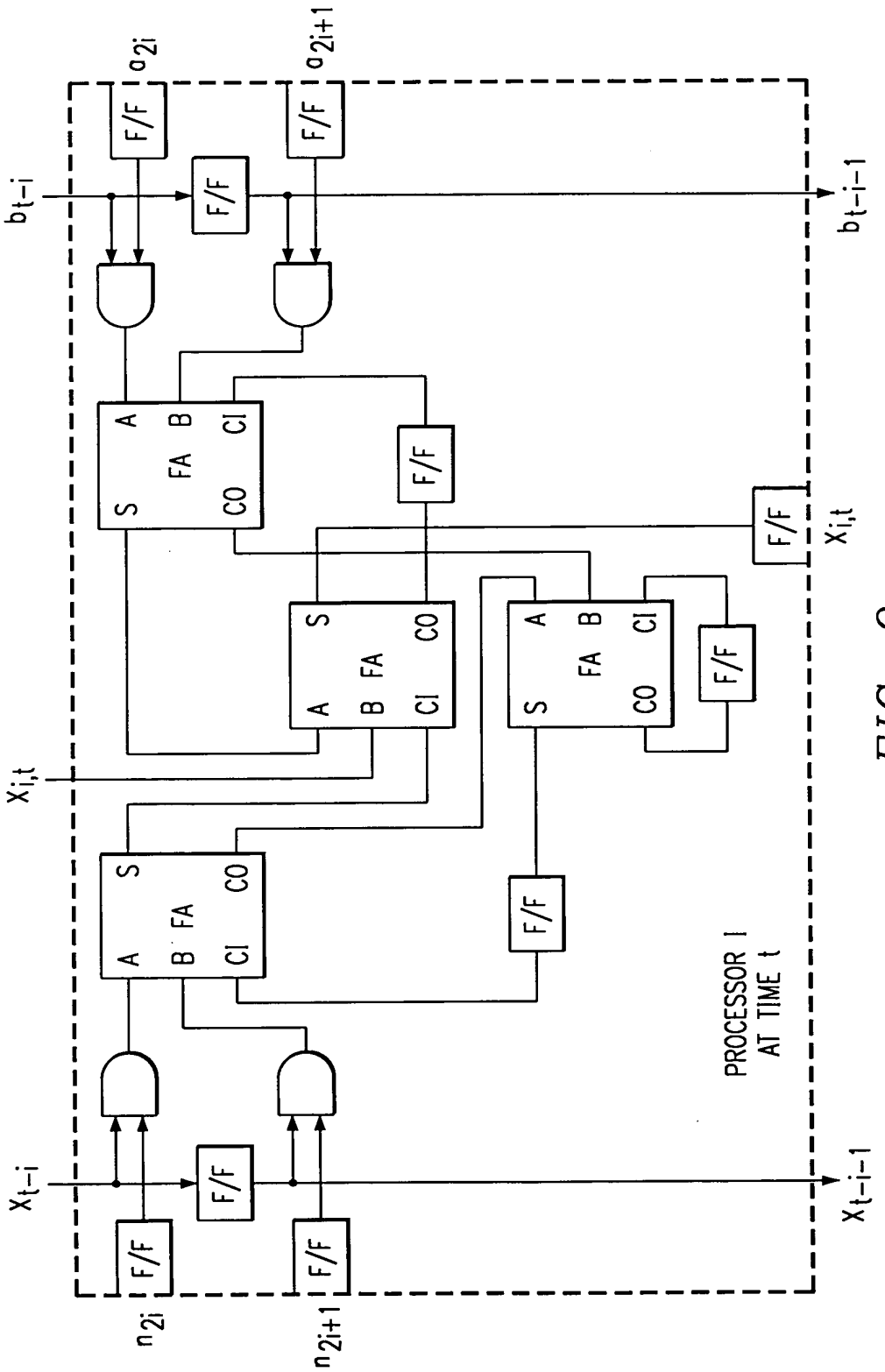
a_{2i}
a_{2i+1}
F/F
b_{t-i}
b_{t-i-1}
A
B
CI
S
FA
CO
$x_{i,t}$
x_{t-i}
x_{t-i-1}
n_{2i}
n_{2i+1}
PROCESSOR I
AT TIME t

FIG. 9

```
Process TypicalBinaryMultiply (A,B)
Z=0;
For i in 0 to n-1 loop
   c := 0;
   For j in 0 to n-1 loop
      Z i+j := (Z i+j +A i *B j +c) mod 2;
      c := (Z i+j +A i *B j +c) div 2;
   end loop;
   for j in n to 2n-1 loop
      Z j := (Z j +c) mod 2;
      c  := (Z j +c) div 2;
   end loop;
   transmit Z i;
end loop;
```

Z_i;

```
Process Reduce(Z i, N)
c := 0;
For i in 0 to n-1 loop
   wait for Z i
   X i := Z i;
   X i := (X i +x*N i +c) mode 2;
   c := (X i +x*N i +c) div 2;
end loop;
X := X/2;
For i in 1 to k-1 loop
   x = X mod 2;  c := 0;
   For j in 0 to n-1 loop
      X j =(X j +x*N j +c) mod 2;
      c =(X j +x*N j +c) div 2;
   end loop;
   X = X/2;
end loop;
```

BITS OF Z FEED SEQUENTIALLY ACROSS

FIG. 10

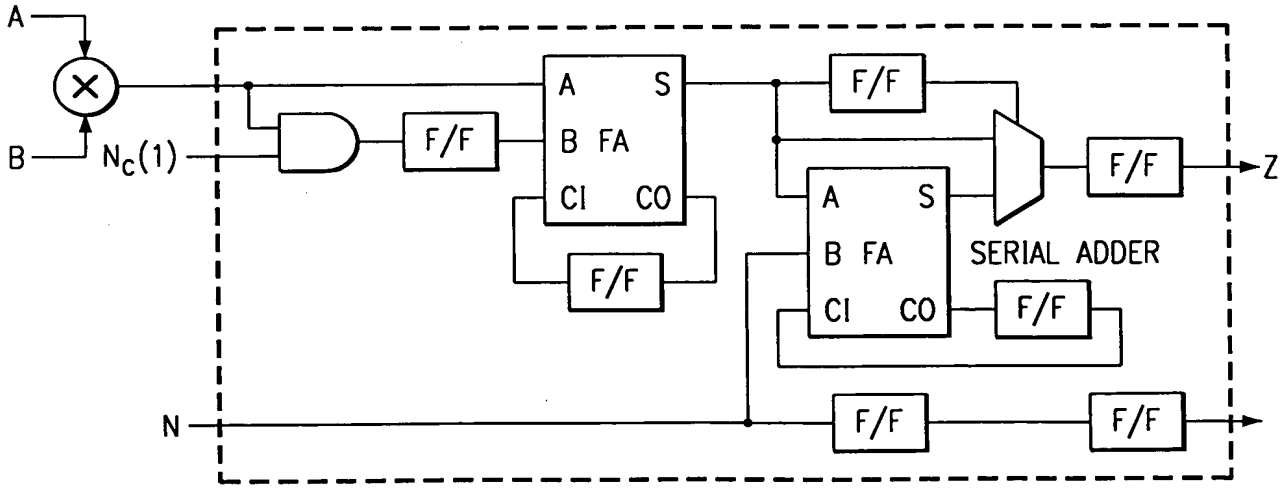

FIG. 18

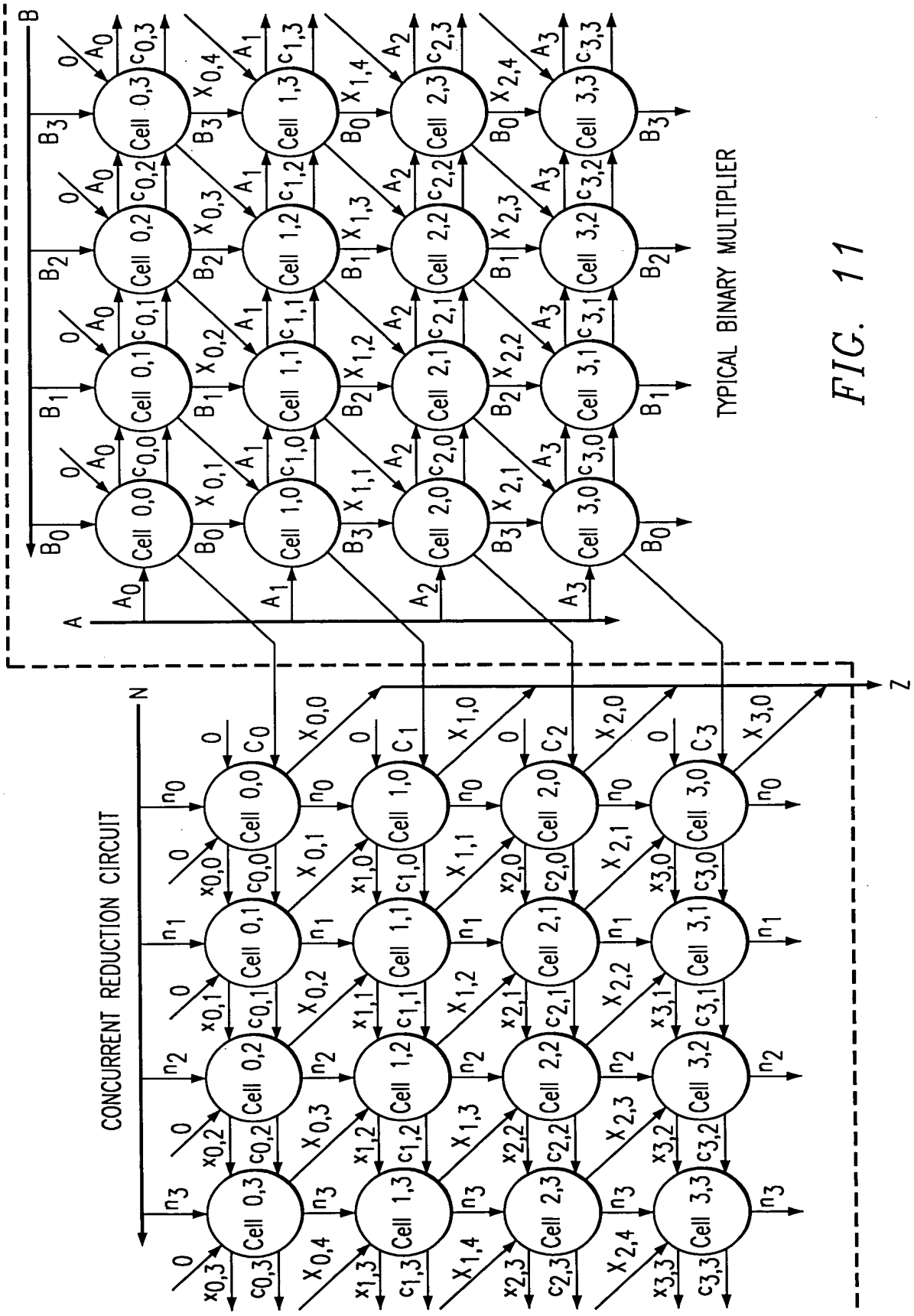
TYPICAL BINARY MULTIPLIER
CONCURRENT REDUCTION CIRCUIT
A
B
N
Z

FIG. 11

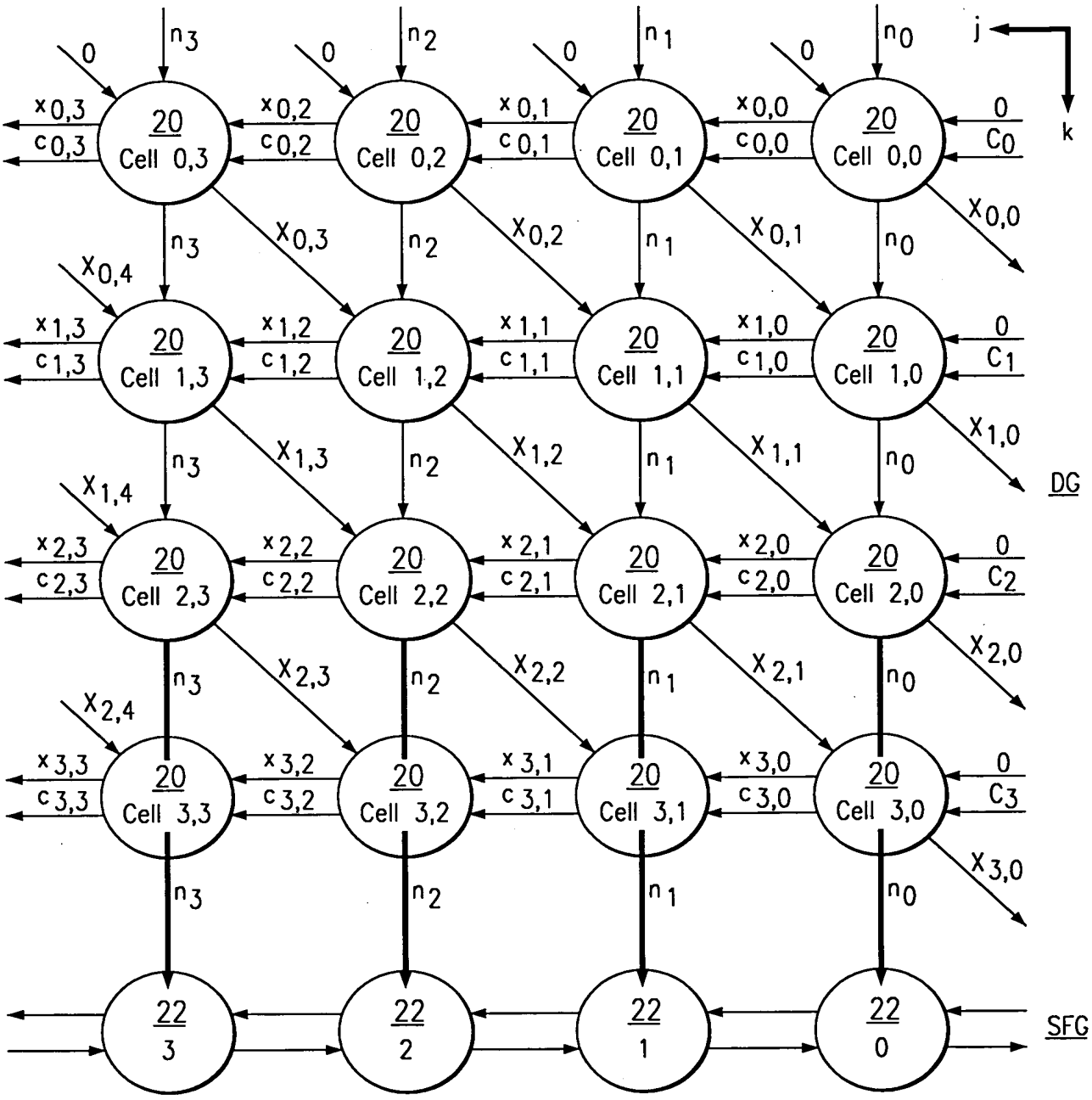
j
k
n3
n2
n1
n0
0
20
Cell 0,3
Cell 0,2
Cell 0,1
Cell 0,0
x0,3
c0,3
x0,2
c0,2
x0,1
c0,1
x0,0
c0,0
C0
X0,0
X0,1
X0,2
X0,3
X0,4
Cell 1,3
Cell 1,2
Cell 1,1
Cell 1,0
x1,3
c1,3
x1,2
c1,2
x1,1
c1,1
x1,0
c1,0
C1
X1,0
X1,1
X1,2
X1,3
X1,4
DG
Cell 2,3
Cell 2,2
Cell 2,1
Cell 2,0
x2,3
c2,3
x2,2
c2,2
x2,1
c2,1
x2,0
c2,0
C2
X2,0
X2,1
X2,2
X2,3
X2,4
Cell 3,3
Cell 3,2
Cell 3,1
Cell 3,0
x3,3
c3,3
x3,2
c3,2
x3,1
c3,1
x3,0
c3,0
C3
X3,0
22
3
2
1
0
SFG

FIG. 12

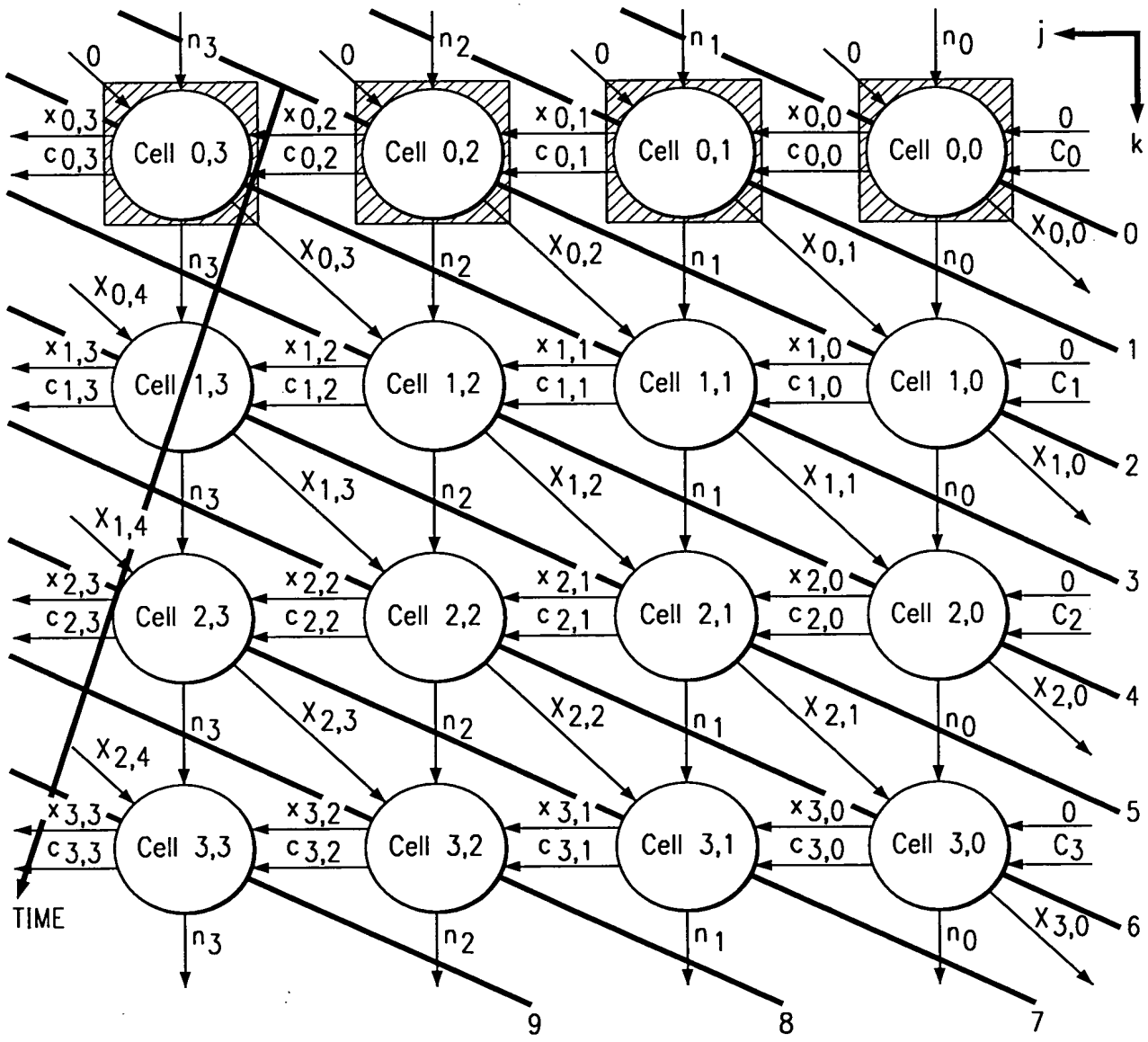
Cell 0,3
Cell 0,2
Cell 0,1
Cell 0,0
Cell 1,3
Cell 1,2
Cell 1,1
Cell 1,0
Cell 2,3
Cell 2,2
Cell 2,1
Cell 2,0
Cell 3,3
Cell 3,2
Cell 3,1
Cell 3,0
TIME
j
k

FIG. 13

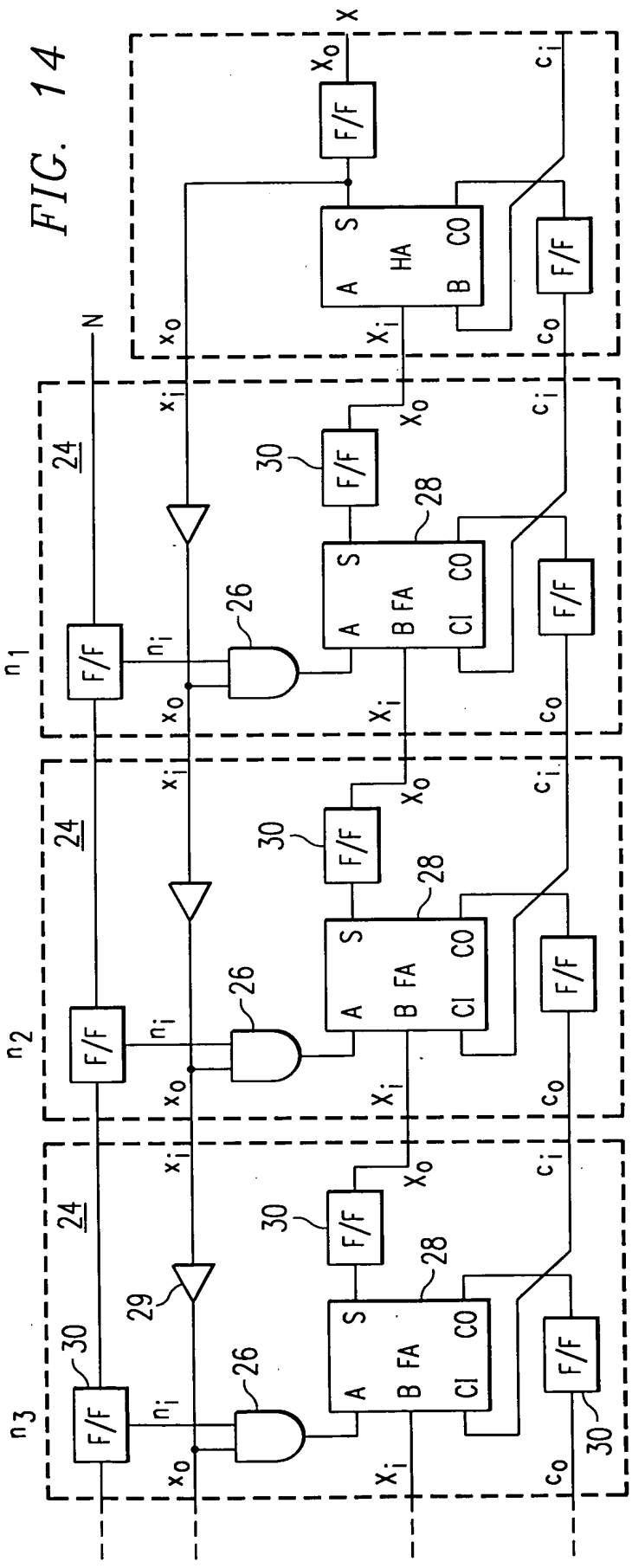
X
N
24
30
28
26
29
F/F
HA
FA
A
B
S
CO
CI
x_o
x_i
c_o
c_i
n_i
n_1
n_2
n_3

FIG. 14

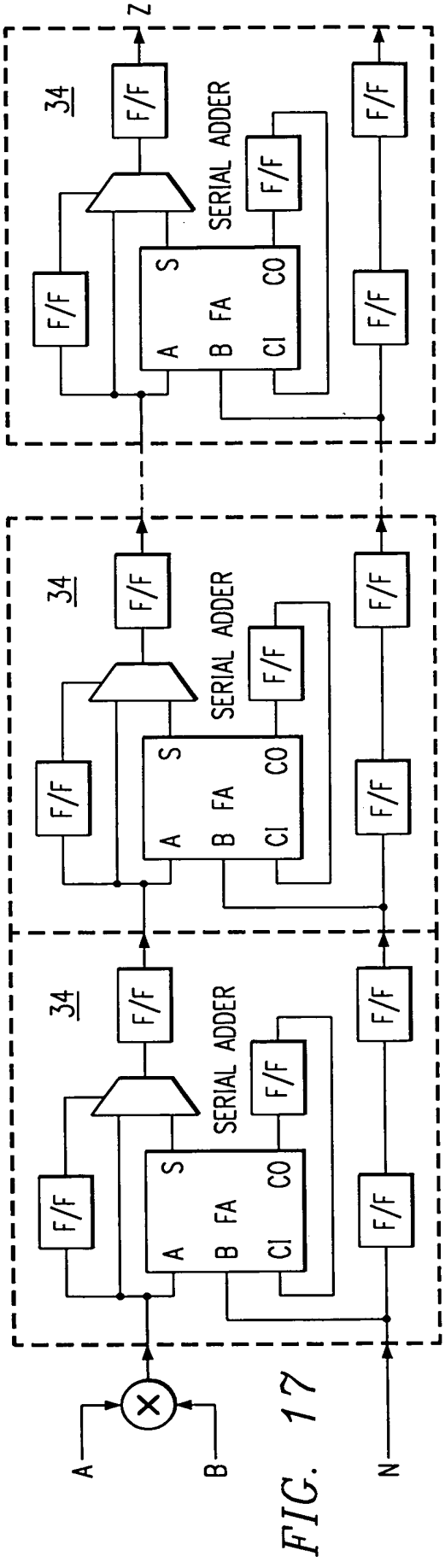
Z
34
SERIAL ADDER
F/F
FA
A
B
S
CO
CI
A
B
N

FIG. 17

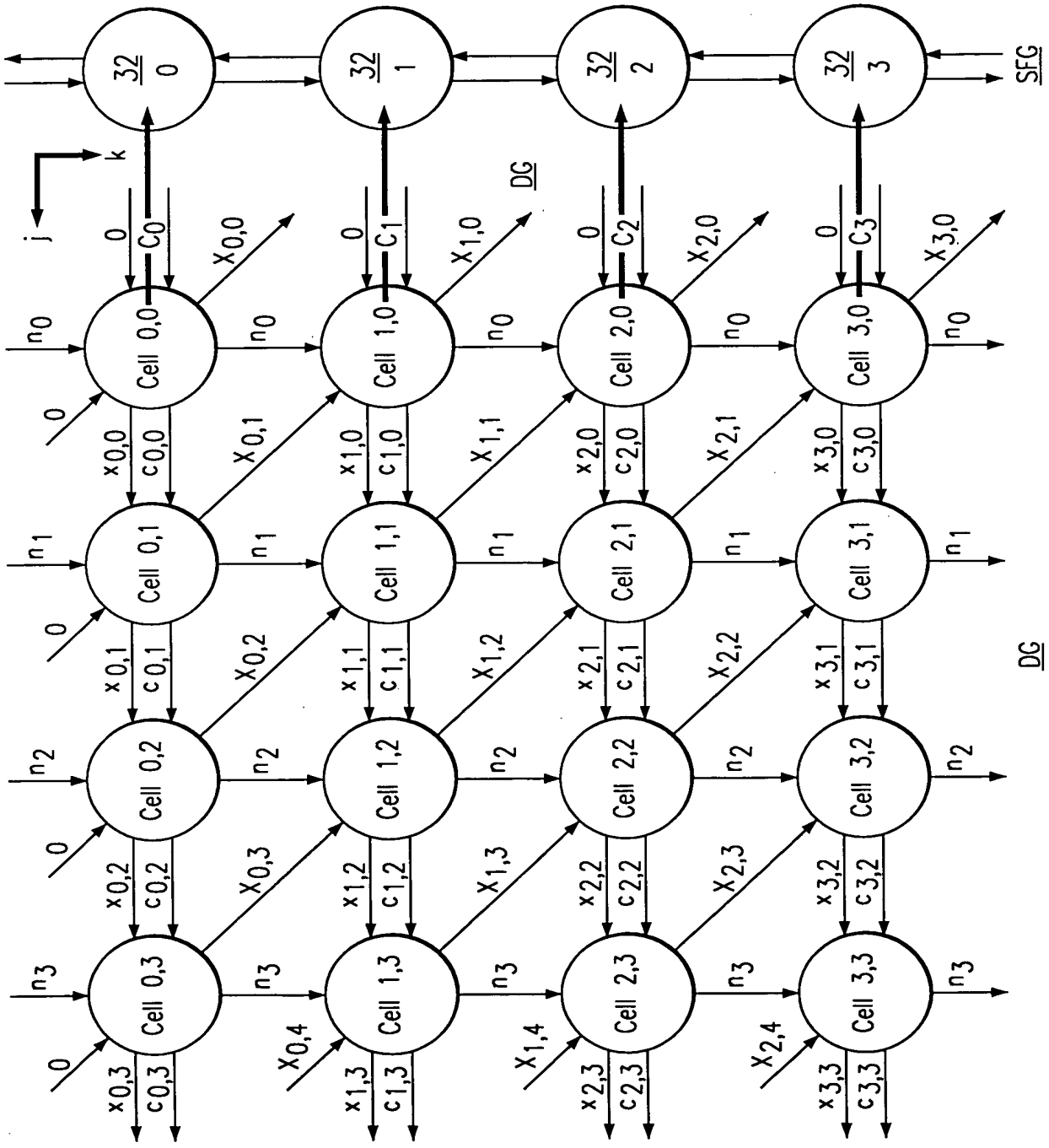
32 0
32 1
32 2
32 3
SFG
DG
DG
k
j
Cell 0,0
Cell 1,0
Cell 2,0
Cell 3,0
Cell 0,1
Cell 1,1
Cell 2,1
Cell 3,1
Cell 0,2
Cell 1,2
Cell 2,2
Cell 3,2
Cell 0,3
Cell 1,3
Cell 2,3
Cell 3,3
C0
C1
C2
C3
n0
n1
n2
n3
0

FIG. 15

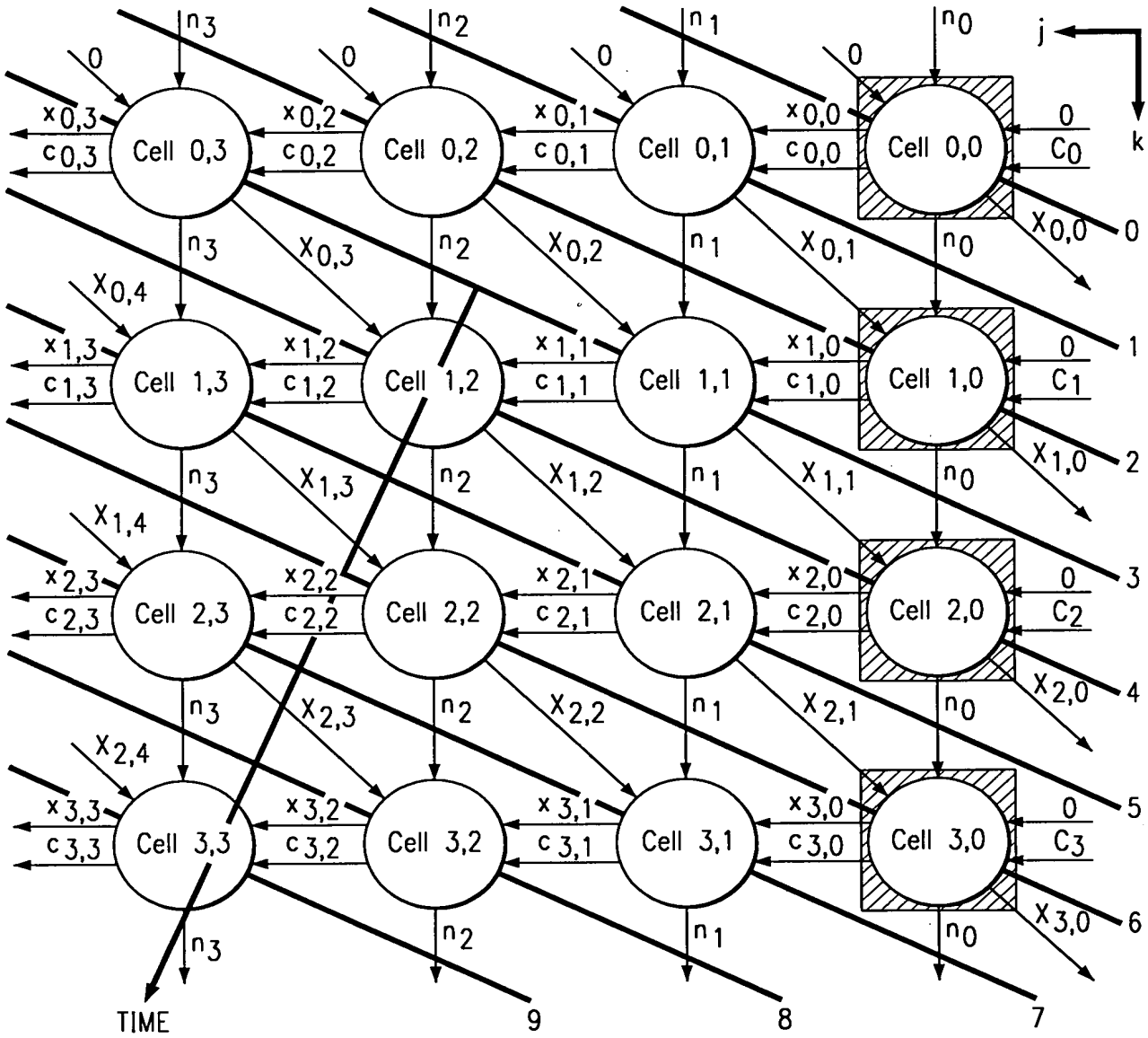
n3
n2
n1
n0
j
k
0
x0,3
c0,3
Cell 0,3
x0,2
c0,2
Cell 0,2
x0,1
c0,1
Cell 0,1
x0,0
c0,0
Cell 0,0
C0
x0,0
x0,4
x1,3
c1,3
Cell 1,3
x1,2
c1,2
Cell 1,2
x1,1
c1,1
Cell 1,1
x1,0
c1,0
Cell 1,0
C1
x1,0
x1,4
x2,3
c2,3
Cell 2,3
x2,2
c2,2
Cell 2,2
x2,1
c2,1
Cell 2,1
x2,0
c2,0
Cell 2,0
C2
x2,0
x2,4
x3,3
c3,3
Cell 3,3
x3,2
c3,2
Cell 3,2
x3,1
c3,1
Cell 3,1
x3,0
c3,0
Cell 3,0
C3
x3,0
x0,3
x1,3
x2,3
x0,2
x1,2
x2,2
x0,1
x1,1
x2,1
TIME
0
1
2
3
4
5
6
7
8
9

FIG. 16

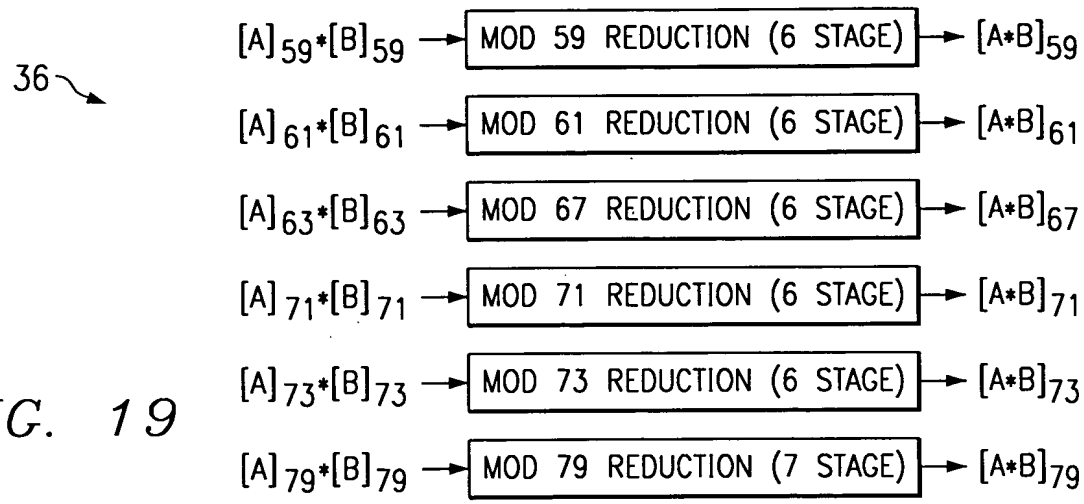

FIG. 19

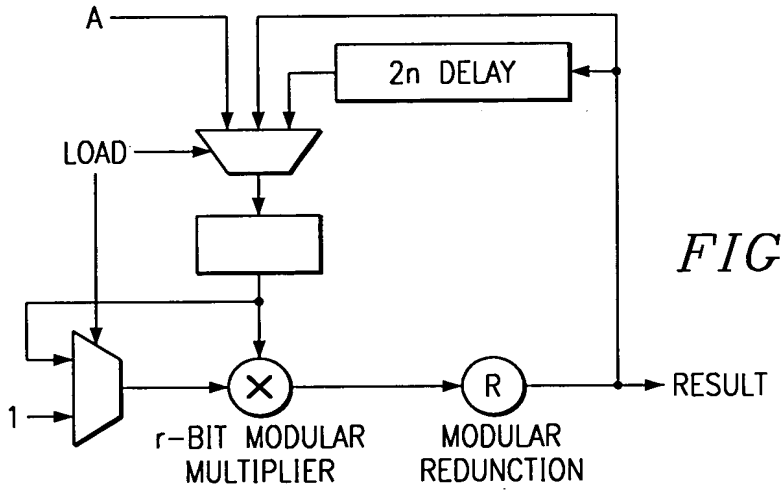

FIG. 20

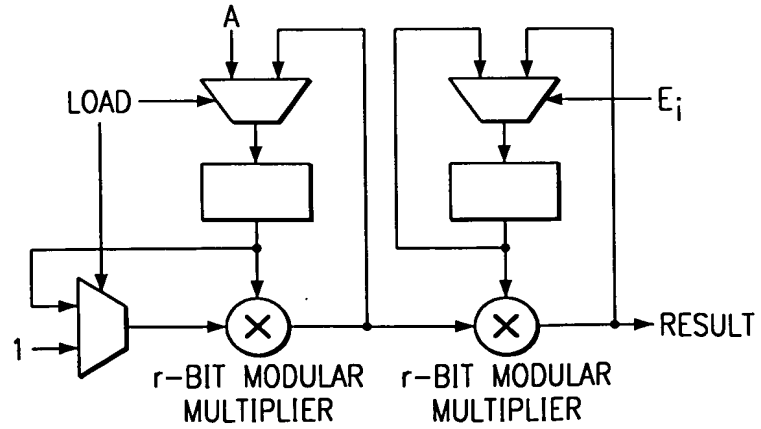

FIG. 21

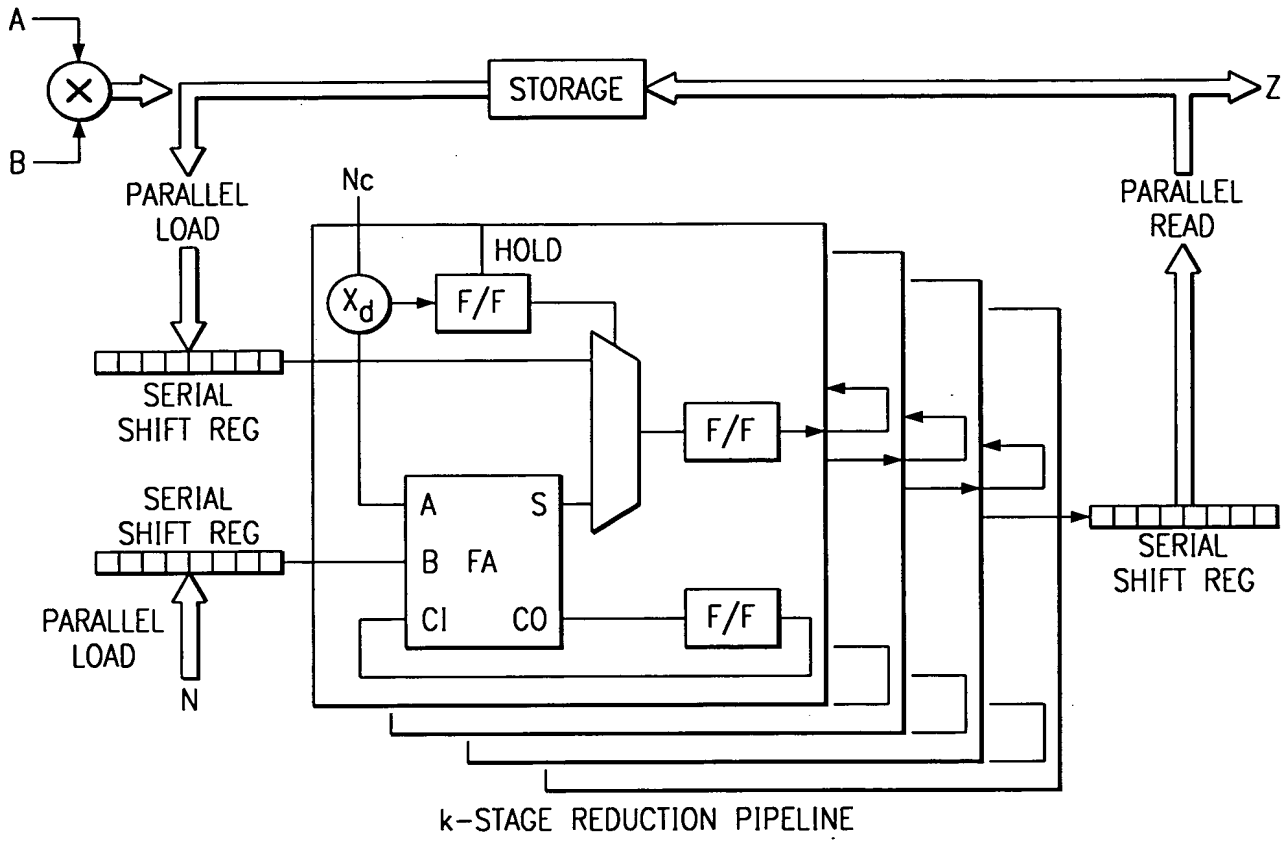
A
B
STORAGE
Z
PARALLEL LOAD
Nc
HOLD
X_d
F/F
PARALLEL READ
SERIAL SHIFT REG
F/F
SERIAL SHIFT REG
A
S
B FA
CI
CO
F/F
SERIAL SHIFT REG
PARALLEL LOAD
N
k-STAGE REDUCTION PIPELINE

FIG. 22

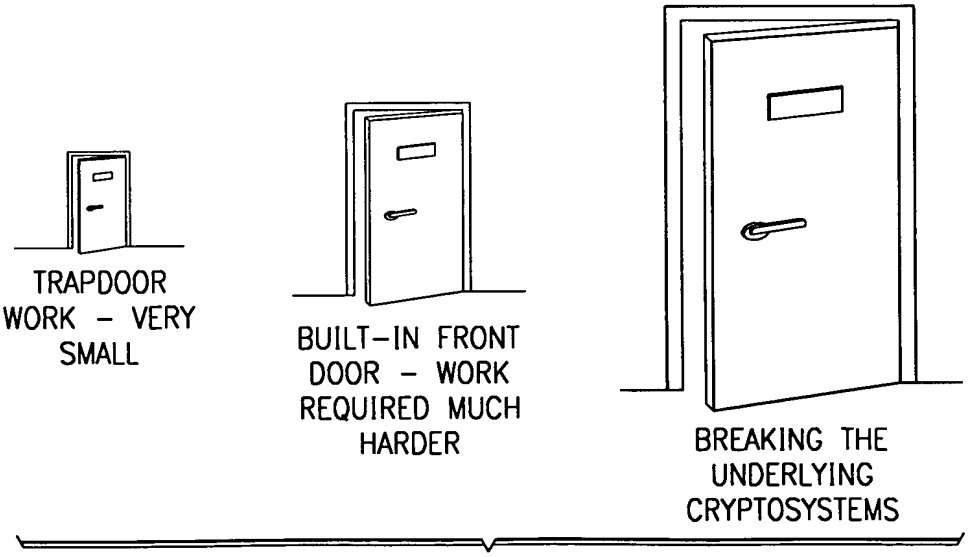
TRAPDOOR WORK - VERY SMALL
BUILT-IN FRONT DOOR - WORK REQUIRED MUCH HARDER
BREAKING THE UNDERLYING CRYPTOSYSTEMS

FIG. 23

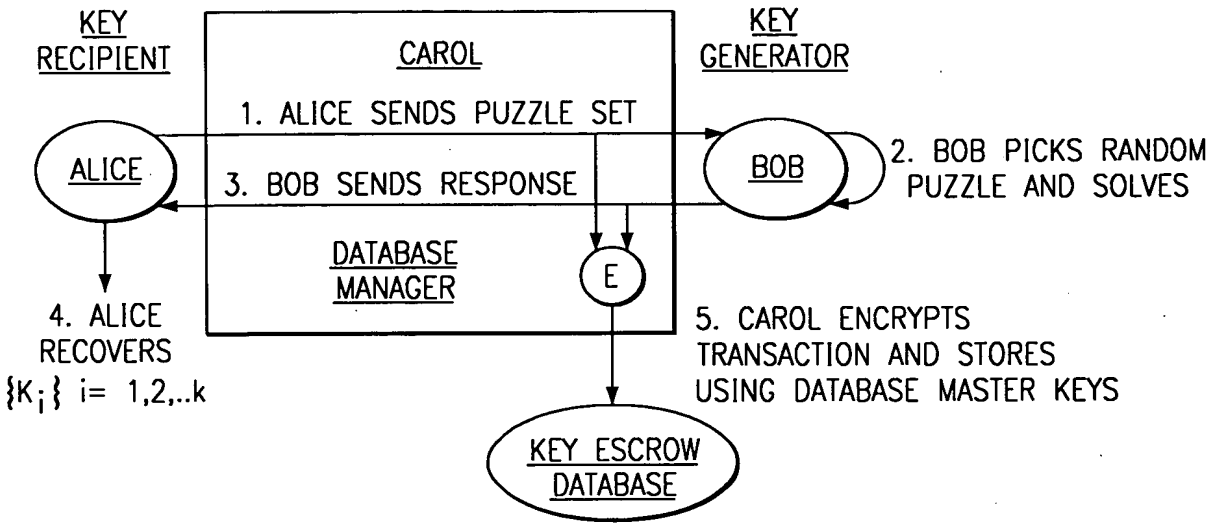
KEY RECIPIENT
CAROL
KEY GENERATOR
1. ALICE SENDS PUZZLE SET
ALICE
3. BOB SENDS RESPONSE
BOB
2. BOB PICKS RANDOM PUZZLE AND SOLVES
DATABASE MANAGER
E
4. ALICE RECOVERS {K_i} i= 1,2,..k
5. CAROL ENCRYPTS TRANSACTION AND STORES USING DATABASE MASTER KEYS
KEY ESCROW DATABASE

FIG. 24

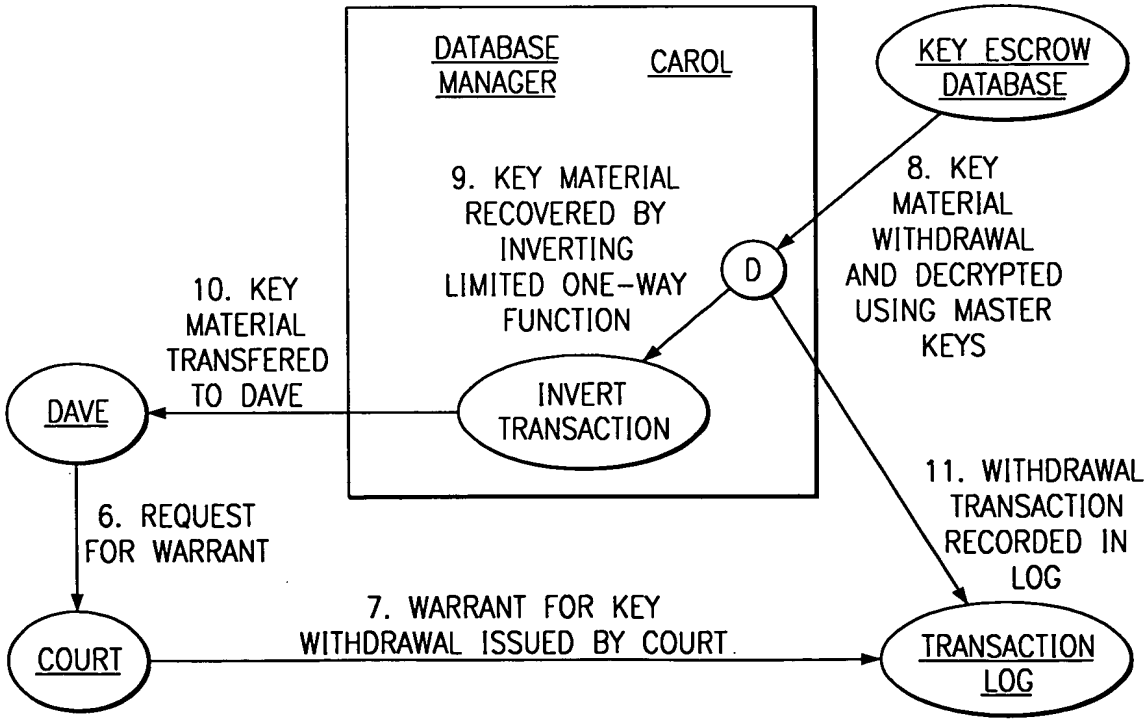
DATABASE MANAGER
CAROL
KEY ESCROW DATABASE
9. KEY MATERIAL RECOVERED BY INVERTING LIMITED ONE-WAY FUNCTION
8. KEY MATERIAL WITHDRAWAL AND DECRYPTED USING MASTER KEYS
D
10. KEY MATERIAL TRANSFERED TO DAVE
DAVE
INVERT TRANSACTION
11. WITHDRAWAL TRANSACTION RECORDED IN LOG
6. REQUEST FOR WARRANT
7. WARRANT FOR KEY WITHDRAWAL ISSUED BY COURT
COURT
TRANSACTION LOG

FIG. 25

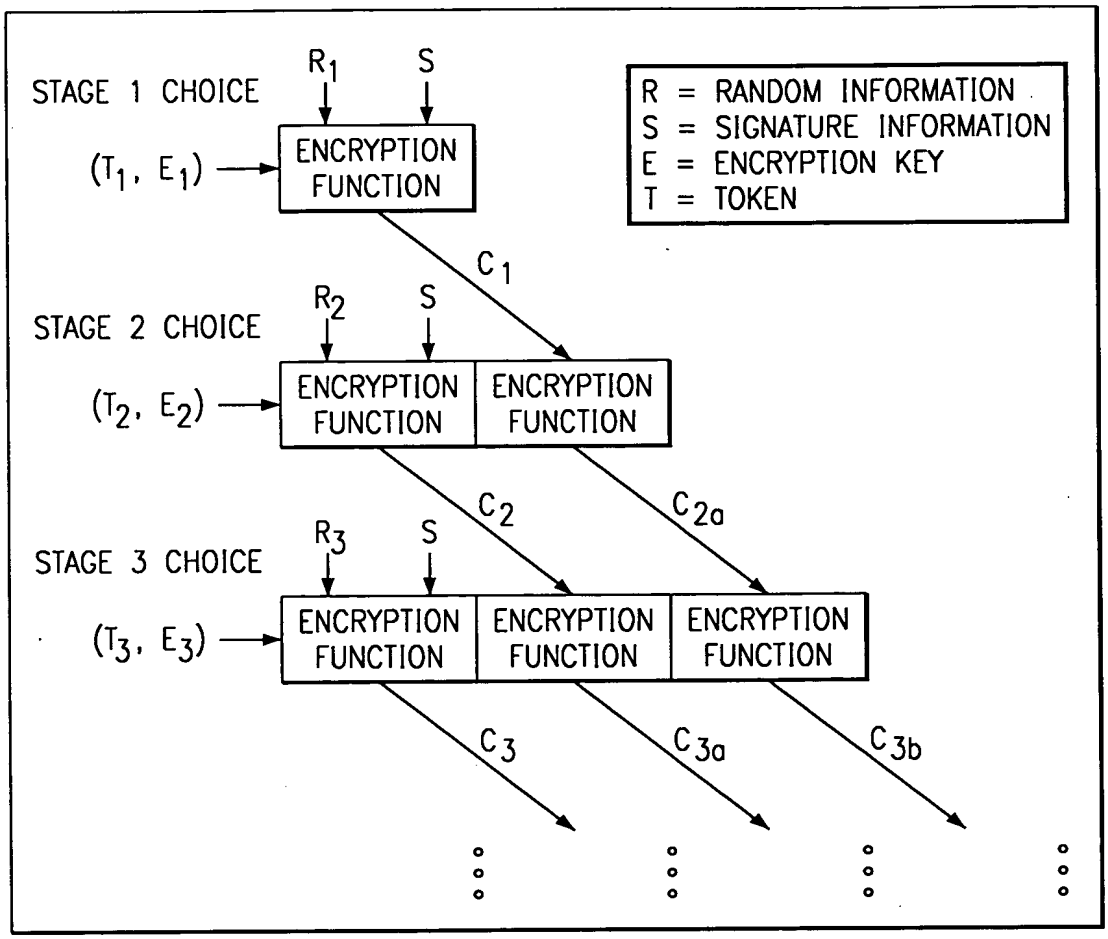
STAGE 1 CHOICE
R_1
S
(T_1, E_1)
ENCRYPTION FUNCTION
R = RANDOM INFORMATION
S = SIGNATURE INFORMATION
E = ENCRYPTION KEY
T = TOKEN
C_1
STAGE 2 CHOICE
R_2
S
(T_2, E_2)
ENCRYPTION FUNCTION
ENCRYPTION FUNCTION
C_2
C_{2a}
STAGE 3 CHOICE
R_3
S
(T_3, E_3)
ENCRYPTION FUNCTION
ENCRYPTION FUNCTION
ENCRYPTION FUNCTION
C_3
C_{3a}
C_{3b}

FIG. 26

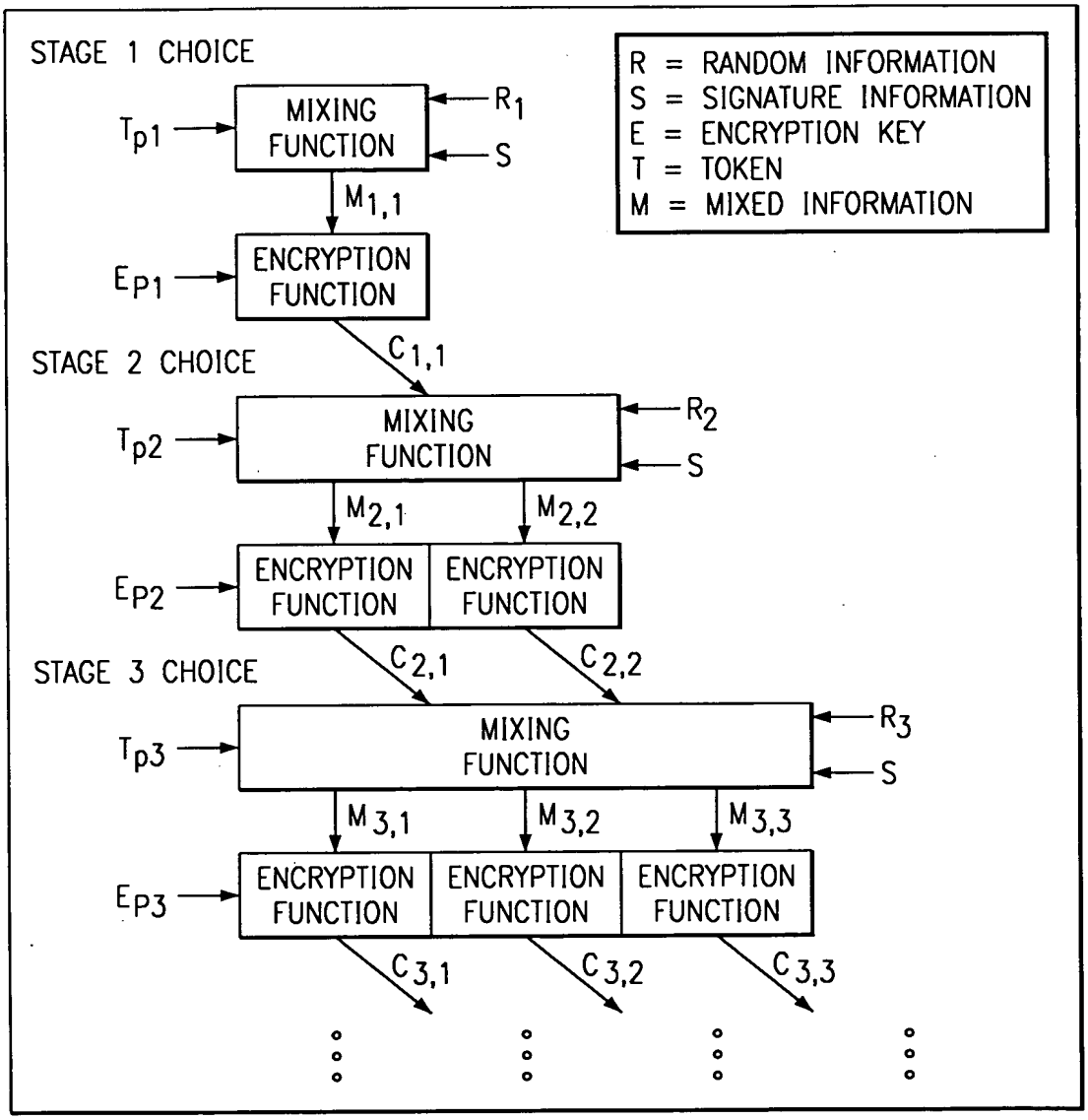
STAGE 1 CHOICE
R = RANDOM INFORMATION
S = SIGNATURE INFORMATION
E = ENCRYPTION KEY
T = TOKEN
M = MIXED INFORMATION
Tp1
MIXING FUNCTION
R1
S
M1,1
EP1
ENCRYPTION FUNCTION
C1,1
STAGE 2 CHOICE
Tp2
MIXING FUNCTION
R2
S
M2,1
M2,2
EP2
ENCRYPTION FUNCTION
ENCRYPTION FUNCTION
C2,1
C2,2
STAGE 3 CHOICE
Tp3
MIXING FUNCTION
R3
S
M3,1
M3,2
M3,3
EP3
ENCRYPTION FUNCTION
ENCRYPTION FUNCTION
ENCRYPTION FUNCTION
C3,1
C3,2
C3,3

FIG. 27